TECHNIQUE T855: UNAUTHORIZED COMMAND MESSAGE

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI	Impair Process Control

Data Sources	
Potential Data Sources	Packet Captures, Network Protocol Analysis, OS Stack Logs, Application Logs
Historical Attacks	Industroyer/CRASHOVERRIDE,[1] Triton Attack at Petro Rabigh[2]

TECHNIQUE DETECTION

The Unauthorized Command Message technique[3] (Figure 1) may be detected if devices are given commands that go outside of their intended function or out of expected order.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[4] and Recipes[5] for asset owners and operators (AOO) to identify indicators of attack for techniques like Unauthorized Command Message within their operational technology (OT) networks. Referencing CyOTE Case Studies[6] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Unauthorized Command Message technique was used in the Industroyer attack in the Ukraine in 2016[7,8] and in the Triton attack at Petro Rabigh in 2017.[9] In these attacks, the following observables were identified:

- An increase of packet traffic

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001

[2] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013

[3] MITRE ATT&CK for ICS, T855: Unauthorized Command Message, https://collaborate.mitre.org/attackics/index.php/Technique/T0855

[4] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.

[5] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.

[6] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.

[7] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[8] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[9] https://www.eenews.net/stories/1060123327

- Increased DMZ traffic between information technology (IT) and OT networks
- Blocking of command messages
- Event logs showing devices performing unexpected functions
- Unfamiliar IP addresses noted in NetFlow logs

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

COMPREHENSION

In the Industroyer attack, the adversary issued unauthorized command messages to devices to change their program state and execute further control of the system. They were able to do this once they had gained access to the Data Historian to initiate the compromise and had begun issuing malicious commands. They were then able to take control of the system and manipulate it to cause impactful and damaging changes.[10]

In the Triton attack, the adversary issued unauthorized command messages as part of their execution of the attack after having moved into the OT network. They first gained access through an engineering workstation to deploy the malware; once they gained control of the workstation, they modified operating modes on devices and modified device logic to issue malicious command messages and shut down part of the plant.[11]

By understanding the nature and possible origins of these attacks, as well as how the adversaries used the Unauthorized Command Message technique to execute the attacks, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE Proof of Concept tool reads a network traffic capture and analyzes it based upon a set of criteria defined in a separate configuration file. The criteria compare the protocol layer fields to static values, alerting on trusted IP lists for unauthorized traffic detection, and validating the Common Industrial Protocol (CIP). This Proof of Concept tool output provides statistics about triggered criteria, such as number of times triggered, which packets caused the trigger, data about the network streams, and which network streams included the full protocol cycle or only a part. The protocol validation summary also identifies the packets associated with validation (or lack thereof).

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor the CyOTE Proof of Concept tool to monitor network traffic for commands issued from a non-authorized device. The tool will use a user-defined list of allowed hosts (in the configuration file) permitted to communicate and provide commands to a device, such as a human-machine interface (HMI) and/or engineering workstation.

[10] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.
[11] CyOTE Case Study: Triton in Petro Rabigh. https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf

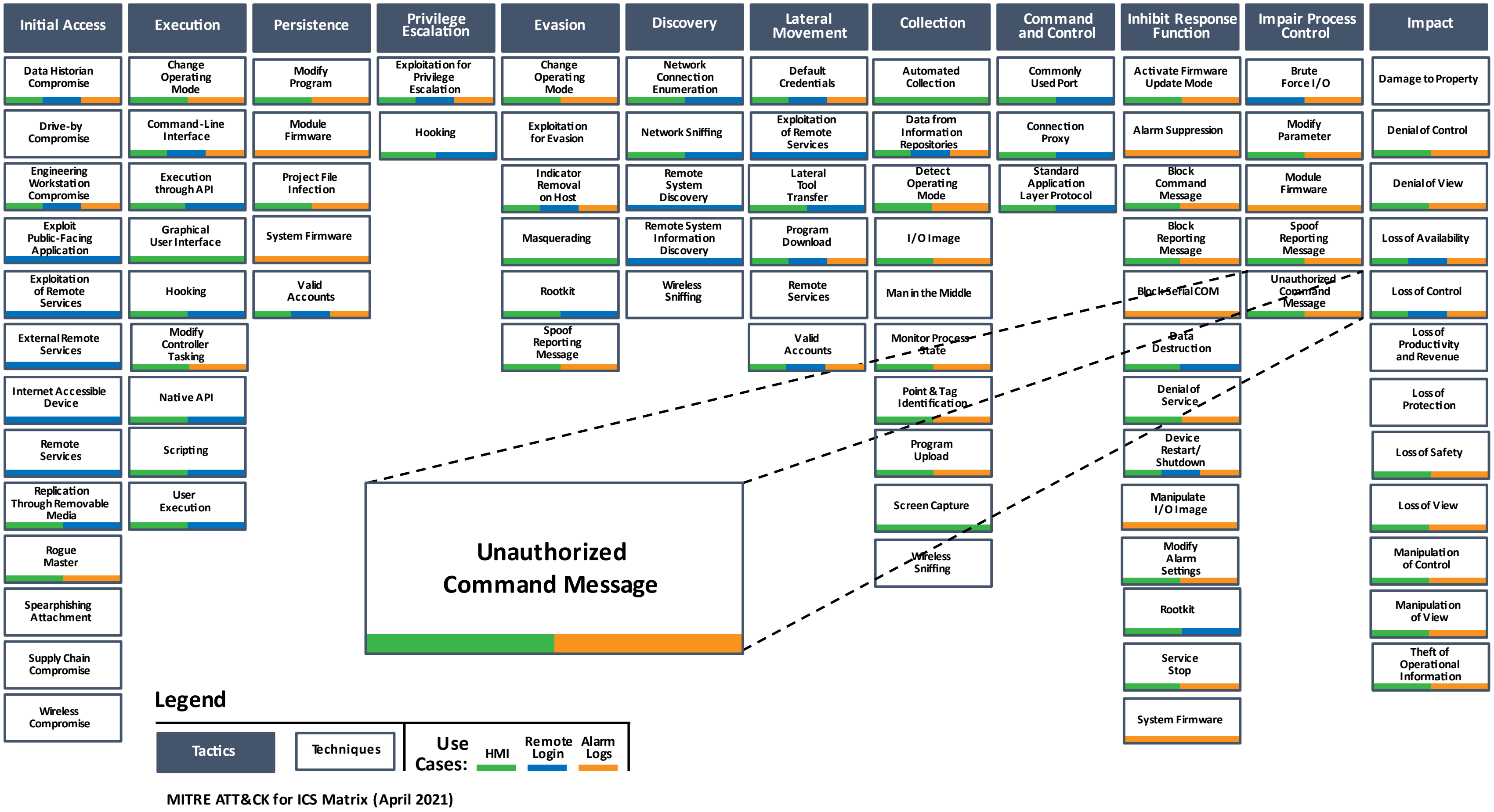
ASSET OWNER DEPLOYMENT GUIDANCE

The CyOTE Proof of Concept tool can be used in a continuously monitoring state by connecting it to a span port of the desired network. This Proof of Concept tool can also be used offline by ingesting network traffic in a Packet Capture (PCAP) file. The operational tool should alert on hosts issuing commands. The command list can be reduced by providing a list of authorized hosts. Alerts can be customized to output to a syslog entry or a STIX 2.1 format.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.

AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

MITRE ATT&CK for ICS Matrix (April 2021)

Figure 1: ICS ATT&CK Framework[12] *– Unauthorized Command Message Technique*

[12] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.